AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Currently amended) A method in a telecommunication system for allowing a SIM-based authentication to users of a wireless local area network who are subscribers of a public land mobile network, the method comprising:

(a) a wireless terminal accessing the wireless local area network through an accessible Access Point;

(b) the wireless terminal discovering an Access Controller interposed between the Access Point and the public land mobile network ~~from the wireless terminal~~;

(c) carrying out a challenge-response authentication procedure between the wireless terminal and the public land mobile network through the Access Controller, the wireless terminal provided with a SIM card and adapted for reading data thereof;

wherein the challenge-response authentication submissions in step (c) take place before having provided an IP connectivity to the user, and are carried:

- on top of a Point-to-Point layer 2 protocol (PPPoE) between the wireless terminal and the Access Controller; and
- on an authentication protocol residing at an application layer between the public land mobile network and the Access Controller; and

the method further comprising:

(d) Access Controller offering the IP connectivity to the user at the wireless terminal, by sending an assigned IP address and other network configuration parameters, once said user has been validly authenticated by the public land mobile network.

2. (Previously presented) The method in claim 1, wherein the step (b) includes establishing a Point-to-Point Protocol session between a Point-to-Point over Ethernet (PPoE) Protocol client in the wireless terminal and a Point-to-Point over Ethernet (PPoE) Protocol server in the Access Controller.

3. (Previously presented) The method in claim 1, wherein the step (c) includes:

(c1) sending a user identifier from the wireless terminal to the public land mobile network through the Access Controller;

(c2) receiving an authentication challenge at the wireless terminal from the public land mobile network via the Access Controller;

(c3) deriving encryption key and authentication response at the wireless terminal from the received authentication challenge;

(c4) sending the authentication response from the wireless terminal to the public land mobile network through the Access Controller;

(c5) receiving at the Access Controller an encryption key from the public land mobile network; and

(c6) extracting the encryption key received for further encryption of communication path with the wireless terminal.

4. (Previously presented) The method in claim 2, further comprising the Access Controller shifting authentication information received on top of the Point-to-Point layer 2 protocol upwards to the authentication protocol residing at the application layer for submissions toward the public land mobile network.

5. (Previously presented) The method in claim 4, further comprising the Access Controller shifting authentication information received on the authentication protocol residing at the application layer downwards on top of the Point-to-Point layer 2 protocol for submissions toward the wireless terminal.

6. (Previously presented) The method in claim 3, further comprising establishing at the wireless terminal a symmetric encryption path by using the previously derived encryption keys at the Access Controller and the wireless terminal.

7. (Previously presented) The method in claim 1, wherein the step (d) includes a previous step of the Access Controller requesting the assigned IP address from a Dynamic Host Configuration Protocol server.

8. (Previously presented) The method in claim 1, wherein the communication between the Access Controller and the public land mobile network goes through an Authentication Gateway of said public land mobile network.

9. (Previously presented) The method in claim 1, wherein the communication between the Access Controller and an Authentication Gateway of the public land mobile network goes through an Authentication Server of the wireless local area network in charge of authenticating local users of said wireless local area network who are not mobile subscribers.

10. (Previously presented) The method of claim 3, wherein the user identifier in step (c1) comprises a Network Access Identifier.

11. (Previously presented) The method in claim 3, wherein the user identifier in step (c1) comprises an International Mobile Subscriber Identity.

12. (Previously presented) The method in claim 1, wherein the authentication protocol residing at the application layer in step (c) is an Extensible Authentication Protocol.

13. (Previously presented) The method in claim 12, wherein the Extensible Authentication Protocol is transported over a RADIUS protocol.

14. (Previously presented) The method in claim 12, wherein the Extensible Authentication Protocol is transported over a Diameter protocol.

15. (Previously presented) An Access Controller in a telecommunication system that comprises a wireless local area network including at least one Access Point, a public land mobile network, and at least one wireless terminal provided with a SIM card and adapted for reading subscriber data thereof, the Access Controller comprising:

a Point-to-Point layer 2 protocol (PPPoE) server for communicating with the wireless terminal over a PPPoE protocol, the PPPoE server being arranged for tunneling a challenge-response authentication procedure; and

an authentication client for communicating with the public land mobile network, wherein the authentication client is configured to implement an authentication protocol residing at an application layer,

wherein the Access Controller is configured to send an assigned IP address and other network configuration parameters to the wireless terminal to provide IP connectivity after the challenge-response authentication procedure is successfully carried out between the wireless terminal and the public land mobile network in the telecommunication system.

16. (Currently amended) The Access Controller in claim 15, ~~wherein~~

wherein the authentication client is configured to shift information received on top of the Point-to-Point layer 2 protocol upwards to the authentication protocol residing at the application layer; and

wherein the PPPoE server is configured to shift information received on the authentication protocol residing at the application layer downwards on top of the Point-to-Point layer 2 protocol (PPPoE).

17. (Currently amended) The Access Controller in claim 16 wherein the Access Controller is adapted for requesting the assigned IP address from a Dynamic Host Configuration Protocol server, after a user has been successfully authenticated by his public land mobile network.

18. (Previously presented) An Access Controller according to claim 17, wherein the Access Controller is adapted for communicating with the wireless terminal via an Access Point.

19. (Previously presented) An Access Controller according to claim 17, wherein the Access Controller is adapted for communicating with the public land mobile network via an Authentication Gateway.

20. (Previously presented) An Access Controller according to claim 17, wherein the Access Controller is adapted for communicating with an Authentication Gateway via an Authentication Server responsible for authenticating local users of the wireless local area network.

21. (Previously presented) An Access Controller according to claim 15, wherein the authentication protocol residing at the application layer is an Extensible Authentication Protocol.

22. (Previously presented) The Access Controller in claim 21, wherein the Extensible Authentication Protocol is transported over a RADIUS protocol.

23. (Previously presented) The Access Controller in claim 21, wherein the Extensible Authentication Protocol is transported over a Diameter protocol.

Claim 24 (Canceled)

25. (Previously presented) A telecommunication system comprising:

a wireless local area network that includes

at least one Access Point,

a public land mobile network,

at least one wireless terminal provided with a SIM card and adapted for reading subscriber data thereof, and

the Access Controller in claim 15 for allowing SIM-based subscriber authentication to users of the wireless local area network who are subscribers of the public land mobile network.